Cybersecurity Assurance

FY17 MID-YEAR PERFORMANCE REPORT[1]

Highlights of the first half of FY17 for the Berkeley Lab Cyber Security Program includes completion of our MFA implementation to meet the September 30th deadline, validation of our MFA implementation by Berkeley Lab Internal Audit Services, continued development of our simulated phishing attacks, participation in an SC Safeguard & Security review of Berkeley Lab's information and cyber security, and hiring a new NLCIO Policy Analyst, Rainier Elias, who will lead and coordinate policy efforts that affect the Labs and Plants.

- **Multifactor Authentication (MFA):** Against a backdrop of evolving requirements and inflexible constraints, Berkeley Lab met the September 30, 2016 Privileged and Standard Users deadline - and did so against a relatively large pool of users. Berkeley Lab's Privileged User implementation, which is unique in DOE, has been the subject of extensive oversight and has leveraged the Lab's CAS assets to provide assurance to DOE regarding this specialized implementation. Berkeley Lab met the original deadline for both Standard and Privileged Users and did so without substantially degrading user-experience or impacting user-flexibility.

- **Safeguard & Security Review:** The triennial Safeguard & Security Review included a cyber and information security review of all of Berkeley Lab, including NERSC and ESnet. This is the first time the Safeguard & Security Review did not utilize previous assessments to satisfy the cyber component. No findings were identified, however Cyber Security received a Noted Strength / Best Practice mention during the outbriefing:

  > *"LBNL is leveraging the BRO IDS in innovative ways to address cyber security risk beyond the conventional scope of intrusion detection. This had made BRO and its supporting infrastructure important to the overall risk profile."*

- **Service**: Berkeley Lab cyber and OCIO also performed extensive service and outreach to DOE as well as the general community this year. Our staff were also actively sought after to speak and inspire the next generation of scientists and cyber analysts and to work with leading cyber researchers to further research into identifying, detecting and combating new cyber risks and threats.

In summary, Berkeley Lab's cyber program has had a very strong start this first half of FY17, reflecting our commitment to excellent risk-management and to broad engagement with our

[1] This report covers the period from September 2016 to March 2017 since the FY 16 Annual Performance Report was submitted in late August 2016.

peers in higher education and DOE to achieve a more science-friendly and secure cyber security environment for research.

RISKS AND MITIGATIONS

Berkeley Lab's overall cyber risk profile continues to primarily remain unchanged. The following three risks still pose the greatest cyber risk to Berkeley Lab:

1. Targeted Phishing,
2. Credential Theft, and
3. Web Servers Vulnerabilities, including SQL injections.

These risks are not unique to Berkeley Lab and are typical cyber risks for any institution. They also do not necessarily pose a greater risk level when compared with other institutions. Berkeley Lab continues to explore new ways to address these risks and to share our results with the greater community.

Targeted Phishing

Targeted phishing is an ongoing cyber security challenge, not only for Berkeley Lab, but for the entire cyber security community. The human factor component of this risk poses an especially unique challenge. Our primary mitigations continue to be user education, detection and preventing privilege escalation. The controls we have in place for these events are continuing to function as anticipated and there continues to be no consequential damage or loss of information..

We are also continuing our simulated phishing attacks that we started last fiscal year. 200 staff members have enrolled in the program and we've completed 4 exercises, Each phishing exercise was also modified to make them more difficult to distinguish from real emails, Individuals can opt-in to receive simulated phishing emails and those who click on the simulated phishing attachments are redirected to awareness material about phishing.

We believe that the phishing exercises have been successful and the feedback that we have received from participants has been positive. We anticipate growing this program throughout the rest of the FY.

Credential Theft

Following last year, Credential Theft continues to be one of our greatest risk. Our existing emphasis on detecting and preventing privilege escalation continues to mitigate this risk. Also like Targeted Phishing, Credential Theft is not unique to Berkeley Lab, it is an ongoing cyber security challenge facing all industries and institutions. Berkeley Lab continues to explore new ways to address this risk by leveraging our expertise in network monitoring and forensics. Multifactor authentication helps in mitigating this risk, however Berkeley Lab has been using multifactor authentication for many of its key systems for several years now, predating the current DOE MFA initiative.

Web Server Vulnerabilities including SQL Injection

Attacks caused by web server vulnerabilities is an ongoing risk facing Berkeley Lab. These attacks can occur via SQL injections, where the attacker sends a web server input that will allow the attacker to subsequently send SQL commands that can be used to manipulate data, such as exposing Personally Identifiable Information. Berkeley Lab performs vulnerability scans to identify web server vulnerabilities, however vulnerable web servers will always exist on our networks. Some vulnerabilities are not fixable and in some cases a web server may be missed by the scans. Berkeley Lab is exploring additional ways to address this risk and is currently evaluating web application firewall products from several vendors.   These tools remain promising in their ability to dynamically protect against attacks without requiring coding changes to thousands of unique science web applications.

Emergent Security Risks and Evolving Threats

Policy and Oversight

The largest single unmitigated risk to Berkeley Lab in the area of cyber security continues to be the risk that compliance-oriented policy will have a negative effect on our cyber program and our core science mission. Funding and expertise for cyber security remain limited resources, so any redirection of those resources reduces the effectiveness of our program.

Ransomware

Malware that encrypts files, requiring victims to pay a ransom to recover the files, is an emerging risk. Known as ransomware, the mechanisms used to infect computers is not new, but the recovery and policy questions raised are challenging. Laboratory Sr. Management has been briefed on this risk as well as the policy decision that may arise if a system becomes infected, the victim has no backups, and the victim desires to pay the ransom.

Existing malware protections, such as antivirus, email filtering, and email deletion capabilities mitigates the overall risk of a ransomware incident to an acceptable level. We have also implemented new Bro policy that can detect ransomware attempting to encrypt files and we have prioritized communication and deployment of new backup solutions and institutional file storage as solutions to recovery. .

Supervisory Control and Data Acquisition (SCADA) systems

We continue to make progress in mitigating cyber security risk associated with SCADA systems. As our understanding of the use of these systems evolves, we have identified two distinct areas to focus our efforts, operational usage and scientific usage.

In the area of operational usage, we have worked with Facilities to prioritize moving SCADA systems to isolated networks, resulting in additional staffing from Facilities to assist in this effort. We have also helped Facilities to mitigate the risk from new purchases of SCADA equipment.

In the area of science, we have conducted a preliminary inventory and assessment of SCADA use by scientists and researchers to refine our overall risk analysis. This inventory and assessment is leading us to publish additional communication and guidance to scientists about the risks and precautions they should take when working with SCADA equipment.

Mirai Botnet

The Mirai botnet is a botnet composed of millions of compromised Internet of Thing (IoT) devices, such as smart thermostats, lightbulbs, etc. While botnets are not a new risk, the size and dynamic nature of the Mirai botnet is creating some operational risk. The risk posed by the Mirai botnet is not unique to Berkeley Lab. Other Labs and Plants are also seeing it affects.

The primary risk posed by the Mirai botnet is not that Berkeley Lab hosts will become part of the botnet. As the botnet scans the Internet for new victims, it creates spikes in host blocking activity that must be addressed by Cyber Security in a timely manner. To help address these spikes, we have recently implemented new host blocking technology and are continuing to explore new countermeasures.

Potential Risk

Staff Recruitment and Retention

Our philosophy of smart cyber security and detection require very smart people who are willing to work across institutional boundaries and develop new tools to accomplish our ends. These people are hard to find and can be difficult to retain, this past year saw a key cyber analyst leave Berkeley Lab for a local startup company. There also continues to be a shortage of qualified cyber staff, especially in the Bay Area where we face stiff competition from Silicon Valley and other institutions.

PERFORMANCE: PEMP GOALS, OBJECTIVES AND NOTABLE OUTCOMES

Communication and Outreach

Berkeley Lab's cyber team continues to provide support to other Laboratory and University sites using Bro, through presentations conferences, and 1:1 consulting with site cyber security teams. We also continue to seek out opportunities to consult with private industry about our cyber program and Bro this year.

So far in FY17, Berkeley Lab cyber has discussed Bro and our cyber approach with:

- Tanium

    - Marist College
    - Jet Propulsion Laboratory
    - John Hopkins University
    - California Institute of Technology
    - Visa, Inc.
    - SLAC
    - University of Michigan

As part of our outreach to the broader community, especially to showcase Berkeley Lab's diversity in cyber, Berkeley Lab cyber has participated in the following community events so far this fiscal year:

- Albany High School career day
- Burton High School girls talk
    - http://www.igniteworldwide.org/news/blog-category/event/philip-and-sala-burton-hs-ignite-panel
- SULI,BLUR,CCI interns Cybersecurity talk September 2016 and January 2017
- Women in Technology Symposium: Recognizing leaders, inspiring the next generation
- America's Summit: Women Entrepreneurs Day @ Facebook
- CNet recognition
    - https://today.lbl.gov/2016/09/21/its-toledano-makes-cnets-most-influential-latinos-in-tech-list/
- TECPUI interview
    - http://tecpui.com/2016/10/03/soledad-antelada-el-rostro-de-la-ciberseguridad-de-berkeley-lab/

In support of DOE's iJC3 effort, Berkeley Lab continues to lead the iJC3 Cyber R&D group and to be a partner in the iJC3 Data Fusion group. The Berkeley Lab iJC3 Cyber R&D effort is being led by Dr. Sean Peisert, however Berkeley Lab cyber will be lending its operational expertise with Bro and data fusion as part of the effort.

The University of California also continues to work with Berkeley Lab cyber on strategies for identifying and preventing cyber breaches and incidents. The Berkeley Lab CIO is part of the select leadership team at UC that is structuring future security improvements for the entire UC system.

DOE Enterprise Defenses

Berkeley Lab's ROE has the CPP Sensor program installed and participates actively in the cyber federated model. Berkeley Lab has indicated its willingness to participate in the DEX program but this program is on hold as it transitions to E3A.

In FY17 we have begun working towards installation of an ODIN sensor on the Lab network and we continue to report all reportable incidents to iJC3.

Multifactor Authentication

Early this FY, Berkeley Lab completed implementation of its Multifactor Authentication Implementation Plan, meeting the DOE deadline for multifactor authentication implementation and achieving 100% compliance for Privileged and Standard Users.

Although our approach does not utilize PIV-I, it does meet the NIST 800-63-2 Level of Assurance requirements for Privileged and Standard Users, is more suitable for an open science environment, is better integrated with our existing cyber program, and provides us with the flexibility to adapt to the changing cyber and risk environment.

Our MFA implementation was assessed by Internal Audit Services early this FY as part of two advisory efforts. The first advisory effort focused on evaluating our implementation plan against DOE MFA and NIST 800-63-2 Level of Assurance requirements. The second advisory focused on evaluating our actual implementation. No findings or concerns about our MFA implementation were identified in either advisory effort.

SIGNIFICANT ACCOMPLISHMENTS

Service

Berkeley Lab CIO continues to play a significant role in National Laboratory CIO efforts to represent the interest of the National Labs at the Federal level. The Berkeley Lab CIO is part of the executive committee of the NLCIO and has led efforts to educate new administration officials through multi-lab reverse site visits to DOE Headquarters. In addition to this leadership role, Berkeley Lab continues to dedicate resources to outreach and best-practice sharing with peer laboratories and research universities, as well as private sector companies, to improve cyber security on the internet.

Multifactor Authentication

Berkeley Lab achieved full compliance with DOE's MFA requirements for Standard and Privileged Users before the end of FY16 deadline and our implementation was successfully reviewed by IAS for compliance with NIST 800-63-2 Level of Assurance and DOE MFA requirements.

INTEGRATED ASSESSMENTS

Assessment Area	Assessment Description	Assessor	Quarter Due	Status of Assessment
IT	Safeguard and Security Review	SC	FY17Q1	Report Pending
IT	OMB Circular A-123 - IT Controls	IAS	FY17Q2	Report Issued
IT	Financial Systems / FISMA Controls Audit	KPMG / OIG	FY17Q3	Planned
IT	Quarterly Review of Cyber Controls	IT	Ongoing	Ongoing

IT	Risk Assessment Self Assessment	IT	FY17Q1	Report Issued
IT	Multifactor Authentication Implementation (Advisory)	IAS	FY17Q1	Report Issued

Integrated Assessment Highlights

An assessment of Berkeley Lab’s information and cyber security was conducted in late January / early February of this year as part of a triennial Office of Science Safeguard & Security Review. The review included a comprehensive assessment of cyber and information security controls for all Berkeley Lab’s enclaves (ROE, BSE, ESnet and NERSC). There were no findings for information security or cyber security, and cyber received the only “Noted Strengths / Best Practices”,

> *“LBNL is leveraging the BRO IDS in innovative ways to address cyber security risk beyond the conventional scope of intrusion detection. This had made BRO and its supporting infrastructure important to the overall risk profile.*”

The final report of the review will be delivered to Berkeley Lab by April 2017.

At the end of FY16, Berkeley Lab CIO requested that Berkeley Lab Internal Audit Services perform an advisory assessment of Berkeley Lab’s Multifactor Authentication Implementation Plan. The goal of this advisory assessment was to provide a third party review of Berkeley Lab’s MFA implementation and to validate meeting NIST 800-63-2 Level of Assurance requirements for Privileged Users and Standard Users as defined in the June 26, 2016 version of the DOE Multifactor Authentication Implementation Approach document.

The advisory assessment was conducted in two parts, the first part focused on Berkeley Lab’s implementation plan and if it met DOE MFA and the NIST 800-63-2 Level of Assurance requirements. The second part focused on the actual MFA implementation. The final report was issued at the end of January 2017. No deficiencies were identified.

Berkeley Lab has been selected this FY by OIG for a Financial System and FISMA controls audit starting in FY17 Q3. The last time that Berkeley Lab had a FISMA control audit was in 2012 and preparations have already begun for this year’s audit. We believe that this will consume a substantial amount of effort from cyber security program during FY17 Q2 and FY17 Q3, especially considering that EA assessed the Lab’s cyber security program during FY16 and had praised our cyber security program.